

CAND

OLL85-1470/1  
12 June 1985

MEMORANDUM FOR: General Counsel  
Director, Office of Security  
Chairman, SECOM  
Director, Office of Information Services/DDA  
Chief, Administrative Law Division/OGC  
Chief, Intelligence Community Affairs/OGC.

FROM:

[Redacted]  
Chief, Legislation Division/OLL

SUBJECT: DoD and DoJ Comments on H.R. 271

1. Attached for your comment and review are DoD and DoJ's draft reports on H.R. 271, Representative Bennett's bill establishing a statutory classification system and providing penalties for unauthorized disclosure of classified information. You will recall that this bill was earlier circulated for comment following the Office of Management and Budget's (OMB) request for Agency views on this proposal. We currently are preparing the Agency response on Representative Bennett's bill which will be available shortly for your review.

2. With respect to the two attached draft reports, DoJ's report on the classification system proposed by Mr. Bennett's bill takes the position that the Executive branch is better equipped than Congress to establish classification criteria and opposes that portion of the bill on this general basis. DoD, on the other hand, states that it has no objection to a statutory classification system and instead has provided very detailed comments on each individual section of the Bennett bill addressing classification. I believe that the Agency should oppose the rigidity and inflexibility that would result from a statutory classification system and should insist that the Executive branch take a uniform position opposing any classification system mandated by Congress which removes needed Executive branch discretion in this area. I would appreciate your comments on this issue.

3. With respect to the leaks portion of the Bennett bill, DOJ, as a general matter, has stated that this type of legislation should be carefully considered by high level

Administration officials before any endorsement of a leaks proposal is made. Justice, in addition, has included a number of arguments against the various affirmative defenses contained in Mr. Bennett's bill. DoD also has a concern with one of these affirmative defenses, although for the most part it defers to DoJ as to the legal sufficiency of the leaks provision contained in the Bennett bill.

4. I would appreciate your comments concerning the attached draft reports by COB, 14 June 1985. If I do not hear from you by this time, I will presume that you have no comments concerning the attached reports. As noted above, our own draft report on the Bennett bill will shortly be sent to you for comment and review.

25X1



Attachments  
as stated

Distribution:

Original - Addressees

- 1 - D/OLL (w/atts)
- 1 - DD/OLL (w/atts)
- 1 - OLL Chrono (w/atts)
- 1 - Leg/Subject - Leaks
- 1 - SWH Signer - (w/atts)

25X1

LEG/OLL:  13 June 1985)

Office of Legislative and Intergovernmental Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

May 30, 1985

Honorable David A. Stockman  
Director  
Office of Management and Budget  
Washington, D.C. 20503

Dear Mr. Stockman:

This is in response to your recent request for the views of the Department of Justice concerning H.R. 271, a bill to amend the National Security Act of 1947 to establish by law procedures for the classification and protection of sensitive information relating to the national security, to provide criminal penalties for the unauthorized disclosure of such information, to limit matters that may be classified and impose penalties for unauthorized classification, and to provide for declassification. The Department of Justice is opposed to the enactment of this bill. While we generally favor legislation prohibiting the unauthorized disclosure of classified information, we think it both inappropriate and unnecessary for Congress to prescribe procedures for the classification and protection of national security information.

First, it is our opinion that H.R. 271 would entail several policy and practical problems which, standing alone, constitute a strong basis for opposing the enactment of this bill.\*/ The Executive Branch, as a matter of policy, is far

---

\*/ It has also been the consistent position of the Department of Justice that the protection of national security information is a primary and fundamental constitutional responsibility of the President that derives from his responsibilities as Chief Executive, Commander-in-Chief, and the principal instrument of United States policy. Although the constitutional powers of the coordinate branches of the Federal Government are often shared even where one branch has primary authority, we are concerned that H.R. 271 would have the effect of limiting the President's constitutional authority to protect sensitive information relating to the foreign relations and national security of the United States as he has deemed necessary in Executive Order 12356. If H.R. 271 were to have such an effect, it might raise sensitive and difficult separation of powers questions.

- 2 -

better equipped than Congress to establish and administer a set of criteria for the classification and declassification of national security information. The Executive possesses the most timely and complete information necessary to determine whether information should be classified to protect the Nation from physical harm or damage to its foreign relations. Moreover, the practical effect of H.R. 271 would be to introduce an element of statutory rigidity into an area that requires flexibility and adaptability in order to respond to the changing circumstances and manifold contingencies of foreign affairs. This process of change and refinement in the criteria for classification is reflected in the issuance of several Executive Orders in recent years governing the classification of national security information, culminating in the issuance of Executive Order 12356 in April 1982.

In particular, Section 502(b)(3) of the bill would weaken the substantive criteria that the Executive Branch has determined should govern classification determinations, by requiring that information could not be classified unless its unauthorized disclosure would cause at least "identifiable damage," whereas currently, information that could reasonably be expected to cause any damage to the national security is classified pursuant to E.O. 12356, Section 1.1(a)(3) and 1.3(b). Further, Section 504(d) would encourage challenges to classification determinations by requiring that any "reasonable doubt" as to the level or propriety of classification should be resolved by applying the least restrictive applicable alternative.

Further, section 509, which would criminalize unauthorized disclosures of classified information, would subject persons who, without authorization, disclose classified information to a foreign government or foreign agent, to life imprisonment or imprisonment for any number of years, and would subject persons who disclose classified information to any unauthorized persons to fines not to exceed \$5,000 and/or imprisonment for not more than one year, or, if the offender had authorized possession of the classified information, to imprisonment for not more than ten years, and/or a fine not to exceed \$10,000.

- 3 -

The decision to endorse a criminal statute concerning the unauthorized disclosure of classified information should be made by high level administration officials, after careful study of the matter, in accord with the agreement reached at an inter-agency meeting chaired by the General Counsel of the Office of Management and Budget, on March 27, 1985. Before endorsing a proposal such as Section 509, the Department would need to determine: (1) the effect of the proposal on existing espionage statutes and related laws, in order to avoid unintended consequences and troublesome inconsistencies; (2) whether the proposed statute would survive constitutional challenges predicated on the First Amendment, and other legal challenges, and (3) whether the provision is redundant or, if not, whether it adequately fills gaps in existing laws that preclude us from prosecuting individuals who willfully disclose national security information without authorization. These issues could be properly assessed only after careful review.

In addition, we question the advisability of including the defenses to prosecution in subsection (d), specifically the defense that the information was not lawfully classified. Presently, in prosecutions under similar statutes (i.e., 50 U.S.C. §783 and 18 U.S.C. §798), the government does not have to prove the legality of the classification. In fact, courts have held that such an inquiry is irrelevant. See, United States v. Boyce, 594 F.2d 1246 (9th Cir. 1979) (prosecution under §798); Scarbeck v. United States, 317 F.2d 546 (D.C. Cir. 1963) (prosecution under §783). This is reasonable because classification itself places the holder of the information on notice of the necessity for pursuing authorized channels for disclosure and because of the problem of revealing additional classified information in the course of proving the validity of the classification of the information that has been disclosed.

Subsection (e) of Section 509 makes the determination of whether the information is lawfully classified a matter of law to be determined by the court. This provision could constitute

- 4 -

a basis for challenges based on alleged violations of due process and the Sixth Amendment right to trial by jury. Whether this provision would be upheld by the courts is uncertain in light of case law holding that all factual issues relevant to guilt or innocence are to be decided by the jury rather than by the court. See, e.g., United States v. Walker, 677 F.2d 1014 (4th Cir. 1982); United States v. Austin, 462 F.2d 724 (10th Cir. 1972); Belton v. United States, 382 F.2d 150 (D.C. Cir. 1967). Further issues exist with respect to Section 509 concerning the lack of a "willfulness" element, the effect of the proposed statute on existing provisions of the law, and whether the coverage of the statute is meant to include recipients of classified information as accomplices, conspirators, or solicitors. Moreover, courts are ill-equipped, and often disinclined to make determinations as to whether, and to what extent, an unauthorized disclosure would damage the national security. See United States v. Hung, 629 F.2d 908, 913-914 (4th Cir. 1980), and cases cited therein.

Subsection (f) of this Section would authorize the Attorney General to seek an injunction against the unlawful disclosure of classified information and would authorize the courts to grant such injunctions upon a showing that a person sought to be enjoined is about to engage in such conduct and that the information was lawfully classified. We believe subsection (f) would be interpreted narrowly to create a statutory right of action in the Attorney General to seek an injunction on behalf of the United States against unlawful disclosures, and not to alter in any way the substantive result reached by the Supreme Court in New York Times Co. v. United States, 403 U.S. 713, 714 (1971). In that case, several Justices commented on the lack of an express statutory prohibition against the publication of information in the circumstances presented. Subsection (f), however, does not purport to provide "limited congressional authorization for prior restraints [tailored to specific] circumstances . . .," such as was suggested by Justice White in his concurring opinion in New York Times Co. See 403 U.S. at 732 (White, J., concurring, joined by Stewart, J.) Therefore, we believe that the only effect of subsection (f) would be to provide to the Executive Branch, by statute, a procedural right of action to seek injunctive relief. We do not believe that such statutory authority is necessary, or that the lack of such express

- 5 -

authority would preclude the Government's seeking an injunction on a particular set of facts, if the substantive burden required by New York Times Co. v. United States could be met. Thus, while the authority provided by subsection (f) might be useful procedurally in that it would eliminate any possible doubts about the Attorney General's authority to seek such injunctive relief, it would not serve to lessen the heavy burden imposed upon the Government in justifying the imposition of such a prior restraint and the actual benefit to the Government may be minimal.

Finally, with respect to the bill's Section 510, we are of the opinion that the present system of administrative sanctions is sufficient to deter improper classification and feel that the fear of criminal sanctions would cause those who make classification decisions to act with excessive caution.

At a minimum, Section 510 should be modified to provide that it is a defense to prosecution that the information in question was properly classifiable or that the classifier believed in good faith that the information was properly classifiable. As presently written, this section can be read to expose the classifier to criminal liability if concealment were one of his motives, even if he believed in good faith that disclosure would harm the national security. If there is to be any criminal liability for improper classification, it should not turn upon the presence of a purpose to conceal, but upon the absence of a good faith belief that disclosure would damage the national security.

Classifying information the disclosure of which would clearly be harmful to the national security could have the secondary effect of concealing incompetence, inefficiency, wrongdoing or administrative errors, or of avoiding embarrassment to individuals or agencies. For example, information concerning an unsuccessful missile test firing may clearly warrant classification, because the disclosure of that information would cause grave damage to the national security, yet the effect of classifying that information might well be to

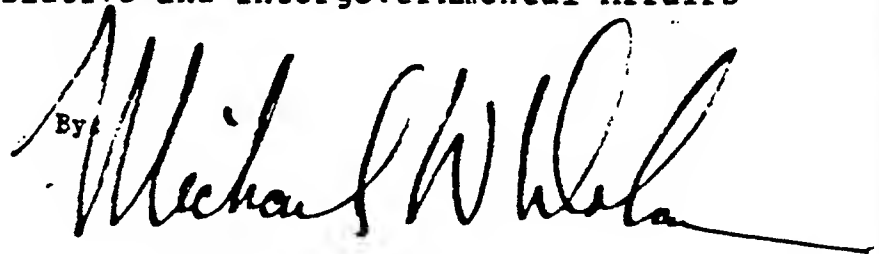
- 6 -

conceal incompetence, inefficiency, wrongdoing or errors by those who carried out the test firing. Indeed, such a concealment may be one of the proper purposes of classifying the information in question; the information that must be concealed from our adversaries may not be that the test firing occurred or the purpose of the test firing, but the error which caused it to fail. Concealment is not wrongful, however, unless it is done for its own sake rather than to protect the national security against damage.

For all of these reasons, but most particularly because of the policy and practical problems associated with this bill, we think it both inappropriate and unnecessary for Congress to enact H.R. 271.

Sincerely,

Phillip D. Brady  
Acting Assistant Attorney General  
Office of Legislative and Intergovernmental Affairs

By 

Michael W. Dolan  
Deputy Assistant Attorney General  
Office of Legislative and  
Intergovernmental Affairs





rn 1-1/85.2

DEPARTMENT OF DEFENSE  
OFFICE OF GENERAL COUNSEL  
WASHINGTON, D.C. 20301

STAT

May 14, 1985

Honorable David A. Stockman  
Director, Office of Management  
and Budget  
Washington, D. C. 20503

Dear Mr. Stockman:

The views of the Department of Defense have been requested on H.R. 271, 99th Congress, a bill, "To amend the National Security Act of 1947 to establish by law procedures for the classification and protection of sensitive information relating to the national security, to provide criminal penalties for unauthorized disclosure of such information, to limit matters that may be classified and impose penalties for unauthorized classification, to provide for declassification, and for other purposes."

Advice is requested as to whether there is objection to the presentation of the attached report to the Committee.

Sincerely,

Werner Windus  
Director  
Legislative Reference Service

Enclosure

Dear Mr. Chairman

Reference is made to your 14 February 1985 request for the views of the Department of Defense on H.R. 271, 99th Congress, a bill "To amend the National Security Act of 1947 to establish by law procedures for the classification and protection of sensitive information relating to the national security, to provide criminal penalties for unauthorized disclosure of such information, to limit matters that may be classified and impose penalties for unauthorized classification, to provide for declassification, and for other purposes."

This Department has no objection to the concept of the establishment of a national security classification system by law. Indeed there is legislative precedent for the establishment of the classification of Restricted Data under the provisions of the Atomic Energy Act, as amended. However, such legislation as proposed by H.R. 271 should not detract from the power and authority of the President to exercise his Constitutional duties, nor should it contain language so restrictive that the capability of the Executive Branch to exercise effective, informed classification management is adversely affected.

H.R. 271 would, among other things: (1) Specify three categories of classification by which national security information may be designated; (2) Vest original classification authority in the President and prescribe how and to what extent such authority may be delegated to other officials in the Executive Branch of the Government; (3) Establish standards for classifica-

tion and categories of information that may be classified; (4) Proscribe classification for certain purposes and authorize administrative disciplinary action for violations; (5) Prescribe the classification designation marking and related data that shall be shown on the face of classified material and mandate the identification of portions of such material that are classified at particular levels and of portions that are not classified; (6) Provide for the protection of classified information furnished to the United States Government by foreign governments or international organizations; (7) Require that national security information be declassified as early as considerations of national security allow; (8) Require the President to prescribe regulations to establish procedures for the systematic and periodic review of all classified information for the purpose of downgrading or declassifying it; (9) Require the President to prescribe regulations to ensure the safeguarding of classified material; (10) Make knowing unauthorized disclosure of classified information a crime punishable by fine and imprisonment and authorize the Attorney General to apply for, and the courts to grant, a permanent or temporary order enjoining such conduct, and (11) make the classification of information for certain purposes a crime punishable by fine and imprisonment.

The Bill departs significantly from Executive Order 12356 in many important particulars and, as drafted, would not provide a legislative base sufficient for an adequately effective system for the identification, classification, protection, review and declassification of information and material relating to the

national security.

Section 501 of the Bill that sets out the purpose of the proposed legislation, would seem to be inconsistent with the provisions of Section 502(b), in that the former recognizes damage to the national security as occurring at only a single level of magnitude. Therefore, it is recommended that line 8 of Section 501 be modified to read: " ... information or material could cause a degree of damage to ...." The recommended changes would make this section of the Bill consistent with Section 502(b), that recognizes three levels of classification, each of which is related to a particular degree of damage.

The Bill makes provision for the designation of original classification authorities by its Section 503(a) in a manner like Executive Order 12356. However, Section 503(a)(3) contains a small defect in that it specifies that an original determination to classify at the Confidential level may be made only by those officials who have been so designated and by those who have original Secret classification authority. As there is no reason to preclude an original Top Secret classification authority from classifying at the Confidential level, it is recommended that the phrase "Top Secret or" be added ahead of "Secret" on line 14, page 4 of the Bill.

The Bill makes no express provision for derivative classification of national security information and thus arguably would require that each act of classification be an original classification decision and be accomplished by an original classification authority. This result is indicated by Section 502(a); 503;

505(a)(2); and 509(g)(4)(A)(iii), and would cause a marked increase in the number of officials exercising original classification authority and a lack of centralized control of classifications throughout the Executive Branch with an attendant loss of classification consistency within and among departments and agencies. Derivative classification, by carrying forward in new documents and material classifications assigned to source information and by use of classification guides, is provided in Executive Order 12356 for the purpose of minimizing those very same problems that had been experienced in administering information security programs under some earlier Executive Orders that made no express provisions with respect to derivative classification. The Department of Defense finds that, in the absence of expressed authority for derivative classification, the Bill is seriously defective.

The Bill provides three designations of classification and defines the categories of national security information to which they shall be applied. The category to which CONFIDENTIAL shall be applied is defined as national security information - the unauthorized disclosure of which reasonably could be expected to cause identifiable damage to the national security. It is this Department's view that the term "identifiable" creates potential litigation problems that may arise if such a quantum standard is applied to the word "damage." Further, in order to determine any of the three degrees of damage called for in the Bill requires an evaluative process in which identification of damage is implied. Therefore, it is recommended that the word

"identifiable" be deleted from Section 501, 502(b)(3), 504(a), and 504(b).

As drafted, the Bill departs significantly from Executive Order 12356, with respect to the matter of foreign government information. While the Executive Order permits the classification of information furnished by a foreign government to the United States under an expressed or implied understanding of confidentiality, the Bill would make a foreign government designation of the information as requiring protection against unauthorized disclosure an absolute prerequisite to classification and protection of it by the United States. Some of our Allies are now extremely concerned that information provided to the United States in confidence (whether or not designated by them as classified) might be subject to forced disclosure under the Freedom of Information Act. As drafted, the Bill will not lessen those concerns. At the same time, the Bill is undesirably broad in permitting classification of information furnished to the United States by an "international organization" without imposing a limitation or qualification concerning the character or membership of such an organization. In order for the Bill to provide adequate basis for classification and protection of foreign government information, the following changes to H.R. 271 are recommended:

a. Section 504. STANDARD FOR CLASSIFICATION:

Subsection (a)(2): Delete the present subsection in its entirety and substitute the following:

"(2) Foreign Government Information;"

b. Section 505. IDENTIFICATION OF CLASSIFIED MATERIAL:

Subsection (c): Delete the present subsection in its entirety and substitute the following:

"(c) Foreign government information shall either retain its original classification designation or be assigned a United States classification designation that shall ensure a degree of protection equivalent to that required by the entity that furnished the information."

c. Section 509. UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION:

Subsection (g)(1)(C): Delete the present subsection in its entirety and substitute the following:

"(C) is foreign government information."

Subsection (g)(4)(C): Delete the present subsection in its entirety and substitute the following:

"(C) is foreign government information as defined in Sec. 511(5)."

d. Section 511. DEFINITIONS: Add the following:

"(5) The term 'foreign government information' means:

(A) Information provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence;  
or

(B) Information produced by the United States

pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof requiring that the information, the arrangement, or both, are to be held in confidence."

As drafted, H.R. 271 also departs significantly from Executive Order 12356 with respect to the matter of classification categories. While the Bill would permit the classification of military plans, weapons, or operations and several other categories of information, no mention is made of other categories as contained in Section 1.3 of E.O. 12356, i.e., "the vulnerabilities or capabilities or systems, installations, projects, or plans relating to the national security," "cryptology," "a confidential source" and the parenthetical phrase "(including special activities)" which appears after "intelligence activities" as contained in Section 1.3(4) of the Executive Order. Executive Order 12356 defines special activities as "activities conducted in support of national foreign policy objectives abroad which are planned and executed so that the role of the United States Government is not apparent or acknowledged publicly, and functions in support of such activities, but which are not intended to influence United States political processes, public opinion, policies, or media and do not include diplomatic activities or the collection and production of intelligence or related support functions." The inclusion of these other categories of information in the Bill would provide a more positive legal basis for



the classification of these types of information, all of which traditionally have been classified because of their sensitivity in that their unauthorized disclosure reasonably could be expected to cause a degree of damage to the national security.

Therefore, the following additions to H.R. 271 are recommended:

Section 504. STANDARDS FOR CLASSIFICATION:

Subsection (a)(3): Delete the comma after "activities" and insert the parenthetical phrase "(including special activities),"

Subsection (a)(7): Renumber to "(10)" and add the following classification categories:

"(7) the vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;"

"(8) cryptology;"

"(9) a confidential source; or"

Section 504(a)(7) would authorize "an official who is the head of an agency" to make a determination that "some other category of information related to the national security ..." would be classifiable. That authorization is overbroad because, as stated it would appear to reach agency heads who have not been designated by the President to exercise authority to originate the classification of national security information. To remedy this, the clause "or by an official who is the head of an agency" should be deleted from lines 7 and 8 of this subsection, and the comma at line 6 should be deleted and the word 'or' inserted instead.

Section 504(b) does not include a presumption of damage

for the unauthorized disclosure of intelligence sources or methods which was added to E.O. 12356 at the recommendation of the Intelligence Community. Therefore, it is recommended that the phrase ", or intelligence sources or methods" be inserted between "source" and "may" on line 11, page 7 of the Bill to ensure proper protection of this category of information.

Section 504(c)(1) of the Bill proscribes classification for certain purposes and makes violators subject to administrative disciplinary action. (Section 510 sets forth criminal penalties for essentially the same violations as noted in the following paragraph.) However, the language of Section 504(c)(1) should make clear that administrative disciplinary action should be taken in the circumstance that an official has willfully classified information in violation of Section 504(c)(1). This Department recommends that the term "willfully" be inserted between "who" and "classifies" on line 20, page 7 of the Bill.

Section 510 would make the classification of information for any of certain purposes a crime against the United States and provide criminal penalties for such classification. Classification for any of the purposes that in Section 510 are made crimes is proscribed and made subject to administrative disciplinary action by Section 504(c)(1) of the Bill. This Department favors enactment of Section 504(c)(1), modified as noted above, and believes that its provisions with respect to administrative disciplinary action will afford ample and effective deterrent to classification for any of the proscribed purposes. This Department believes there now is no real need for enactment of criminal

penalties in order to deter classification for any of the purposes recited in Section 510 and for that reason is opposed to enactment of Section 510 of the Bill at this time. At a minimum, the term "willfully" should be inserted between "Whoever" and "classifies" in the first sentence of Section 510 in order to ensure that intent is an element of the offense and "violations of law" should be inserted between "conceal" and "incompetence." This latter addition will make this Section, if retained, consistent with Section 504(c)(1).

Section 504(c) of the Bill should be expanded to include an additional limitation on classification so that there is no legal question about the authority of the Executive Branch to reclassify information in particular circumstances. A new Section 504(c)(4) should be added to read:

"(4) Information may not be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), unless such classification or reclassification meets the requirements of Section 504 and is accomplished personally and on a document-by-document basis by the agency head, the deputy agency head, the senior agency official responsible for the information security program, or an official with original Top Secret classification authority."

Section 504(d) of the Bill makes use of a concept from Executive Order 12065 that is biased in favor of "openness in government" in that it would require that information not be

classified when there is doubt about the need for classification. The Department recommends that the Bill be modified to eliminate this bias by adopting the more neutral, and safer, language of the current Executive Order. The following is suggested:

"(d) If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by an original classification authority, who shall make this determination within a reasonable period of time, normally 30 days. If there is a reasonable doubt about the appropriate level of classification, the information shall be safeguarded at the higher level of classification pending a determination by an original classification authority, who shall make this determination within a reasonable period of time, normally 30 days."

Section 505(a) of the Bill, in specifying that each item of classified "material" show the "identity" of the official authorizing the original classification, would impose a costly administrative burden of little, if any, benefit in all applications. While recognizing the requirement is sound and useful if it is applicable only at the time of original classification and only with respect to paper copies of documents, this Department is opposed to the necessity to mark each and every item that would result from the present language of this section. Additionally, as drafted this section can be construed as both requiring that the official authorizing the original classification be identified by name and precluding identification by title of position held. In this Department, original classification authority is

delegated to officials by title of position held. This is due to the frequency of rotation of officials assigned to such positions. It is the experience of the Department that a requirement to show the "identity" of the official authorizing an original classification will not be directly useful. Moreover, this section would require that classified material be annotated to show both the date of its preparation and the date of its classification. A literal application of this requirement usually would result in three dates appearing on a typical place of classified correspondence, and the date it was signed. The latter date is required by common business practice. In cases of original classification, all these dates typically are very close if not the same and hence the present language of this section imposes a requirement for which there is no real need.

In order to free the Bill of these burdensome requirements, the following changes in H.R. 271 are recommended:

Section 505. IDENTIFICATION OF CLASSIFIED MATERIAL:

Subsection (a): Delete the present subsection in its entirety and substitute the following:

- (a) At the time of original classification, the following shall be shown on the face of paper copies of all classified documents:
  - (1) One of the three classification designations specified in Section 502;
  - (2) the identity of the original classification authority if other than the approving or signing official;
  - (3) the agency or office of origin; and

- (4) the date or event for declassification or the notation 'originating agency's determination required'."

Section 505(b) could be construed as requiring that all portion markings must appear on the "face," i.e., first page of a document and, further, that classified equipment and weapons bear portion markings. Such requirements would be useless and unreasonable in practice. The following change is recommended:

Subsection (b): Delete the present subsection in its entirety and substitute the following:

"(b) Each classified document shall, by marking or other means, indicate clearly which portions are classified, with the applicable classification designation, and which portions are not classified. The President may waive the requirements of the preceding sentence for specified classes of documents or information."

While the Department of Defense does not oppose the concept of Section 505(d), and in fact presently has a viable "challenge" program in place, it is our view that this level of detail would more properly be placed in implementing Presidential directives.

Sections 506(a) and (b) provide that declassification of classified information shall be given emphasis comparable to that afforded classification of national security information, and are redundant to established legislative policy, embodied principally in the Freedom of Information Act (5 U.S.C. 552), which already provides for the protection of rights of public access to government information. Thus, it is recommended that the first sentence of Section 506(a) and the last sentence of Section 506(b)

be deleted.

A further change to Section 506(b) is needed to avoid a possible interpretation that classified information in the possession of agencies such as the Department of Defense must be physically reviewed on some periodic basis for the purpose of determining whether downgrading or declassification of that information is possible. Such a practice would be extremely labor intensive and with little or no benefit. To eliminate this area of concern, and to incorporate a related useful feature of Executive Order 12356, it is recommended that the word "periodic" be deleted from line 6 on page 10 of the Bill and be replaced with "mandatory." The present mandatory declassification review provisions continue to be a useful alternative to the Freedom of Information Act as a means of getting particular information declassified.

With the above recommended changes, deletion of records management language that is not directly related to the purpose of the Bill, and editorial adjustments, the balance of Sections 506(a) and (b) should be combined into a new Section 506(a) that would read as follows:

"Sec. 506. (a) Information classified under this title or under a prior Executive order authorizing the classification of national security information shall be declassified as early as considerations of national security allow. The President shall prescribe regulations to establish procedures for the systematic and mandatory review of all such classified information for the purpose of declassifying it

at the earliest practical date."

A new Section 506(b) should be added to the Bill that would clarify the conditions under which information is declassified. Its addition will serve to provide a legal basis for continued classification of information in appropriate circumstances when there has been an unauthorized disclosure of that information. This new Section 506(b) would read as follows:

"(b) Information classified in accordance with Section 504 shall not be declassified automatically as a result of any unofficial publication or inadvertant or unauthorized disclosure in the United States or abroad of identical or similar information."

Section 507(a)(1) is not clear with respect to the matter of who will determine that a person is trustworthy. It is the view of this Department that such determinations must reside with the employing agency. To clarify this, it is recommended that Section 507(a)(1) be amended by inserting the words "by the agency concerned" between the words "determined" and "to." This change also will make the Bill similar to current Executive Order 12356 provisions.

Section 507(a)(5) of the Bill as drafted would require accountability records for all classified information, and could be construed as imposing an inflexible requirement for costly measures that are not universally necessary for effective protection. It is recommended that the wording of this subsection be changed to read "(5) appropriate records to assure control or accountability for all classified information ..." so that cost-



effective alternatives may be utilized.

This Department believes that it is necessary to further amend Section 507 in order to make clear that security clearance determinations made by Executive Branch agencies such as the Department of Defense are not reviewable in the courts or by the Merit Systems Protection Board except to ensure agency compliance with its own established procedures. The Department of Defense is suffering currently from what is believed to be wholly unintended judicial and quasi-judicial second guessing in this area. To remedy this, it is recommended that subsection (c) be added at the end of Section 507 that would read as follows:

"(c) Notwithstanding any other provisions of law, the security and security clearance determinations made by an Executive Agency pursuant to subsection (a)(1) are final, committed to agency discretion by law, and not reviewable by courts or the Merit Systems Protection Board except to ensure compliance with prescribed agency procedures."

It is recommended that Section 508 be revised by adding at the end of the present text additional wording as follows:

", as amended, and regulations issued pursuant thereto" because the Atomic Energy Act of 1954 does not itself address classification, downgrading or declassification of material designated as Restricted Data or Formerly Restricted Data.

In order to ensure consistency between H.R. 271 and Title 18, U.S.C., Section 798, Disclosure of Classified Information, which deals with cryptologic information, devices, and materials, the current Section 508 should be retitled "Material Covered by

Other Statutes;" the current Section 508 should be redesignated Section 508(a), and a new Section 508(b) added which reads as follows:

"(b) Cryptologic information, devices and materials specifically designated as such in accordance with Title 18, U.S.C., Section 798, shall be protected and unauthorized disclosures may be prosecuted under the provision thereof, provided, however, that cryptologic information also may be protected under the provisions of Section 509(f) of this statute."

Section 509 would make certain knowing communications of classified information crimes against the United States and provide criminal penalties for such unauthorized disclosure. Certain defenses to prosecution under this section also are provided. One such defense (Section 509(d)(1)) is that the information communicated had been publicly disclosed before the commission of the offense with which the defendant is charged. It is the view of this Department that an instance of public disclosure of classified information that is not in fact or in law an official public disclosure should not be made to constitute a statutory defense to prosecution under subsections (b) and (c) of this section. Accordingly, it is recommended that Sections 509(a), (b) and (c) be amended to add ", willfully, or negligently" between the words "knowingly" and "communicates," and that Section 509(d)(1) be changed to read "(1) before the commission of the defense ... publicly disclosed officially;". This Department favors enactment of criminal penalties as are provided in Section

509 of the Bill but subject to the foregoing defers to the Department of Justice with respect to the style and legal sufficiency of the language of the Bill.

The Department notes, without making a recommendation, that Section 509(d)(3) of the Bill makes it a defense to prosecution that the information was communicated only to Congress. Such a communication, as specified in this Section, is not an unauthorized disclosure of classified information and thus would not be a crime.

It is of concern to this Department that H.R. 271 provides no specific legislative authority concerning access and control, distribution and safeguarding of particularly sensitive information. The Congress previously has singled out the protection of intelligence sources or methods and classified cryptologic information, including communications intelligence, as being of special concern to it. It would be consistent with earlier Congressional action and useful to the Executive Branch to include in H.R. 271 provisions with respect, respect to special access programs. The following is suggested:

"SPECIAL ACCESS PROGRAMS:

Sec. . Agency heads authorized to originate the classification of information as 'Top Secret' pursuant to Section 503(a)(1) of this title may create special access programs to control access to and distribution and safeguarding of particularly sensitive information classified pursuant to this title or prior Executive Order governing the classification of information in the interest of nation-

al security. Such programs may be created or continued only by written direction of such an Agency head, except that for cryptologic information, such programs may be created or continued only by the Secretary of Defense and for intelligence activities (including special activities but not including military operational, strategic and tactical programs), or intelligence sources or methods, only by the Director of Central Intelligence, and only on a specific showing that:

(a) normal management and safeguarding procedures are not sufficient to limit need-to-know or access;

(b) the number of persons who will need access will be reasonably small and commensurate with the objective of providing extra protection for the information subject to the special access program;

(c) the special access controls balance the need to protect the information against the full spectrum of needs to use the information."

The Department of Defense believes there is and will continue to be need for an orderly and effective system for identification and protection of information that requires protection in the interest of the national defense or foreign relations of the United States and does not oppose enactment of a broad legislative base for such a system. With modification and revision of certain particulars as recommended herein, the Department of Defense does not oppose enactment of H.R. 271.

The Office of Management and Budget advises that, from the

standpoint of the Administration's program, there is no objection to the presentation of this report concerning H.R. 271 for the consideration of the Committee.

Sincerely,

99TH CONGRESS  
1ST SESSION

# H. R. 271

To amend the National Security Act of 1947 to establish by law procedures for the classification and protection of sensitive information relating to the national security, to provide criminal penalties for unauthorized disclosure of such information, to limit matters that may be classified and impose penalties for unauthorized classification, to provide for declassification, and for other purposes.

---

## IN THE HOUSE OF REPRESENTATIVES

JANUARY 3, 1985

Mr. BENNETT introduced the following bill; which was referred jointly to the Committee on Armed Services and the Permanent Select Committee on Intelligence

---

## A BILL

To amend the National Security Act of 1947 to establish by law procedures for the classification and protection of sensitive information relating to the national security, to provide criminal penalties for unauthorized disclosure of such information, to limit matters that may be classified and impose penalties for unauthorized classification, to provide for declassification, and for other purposes.

- 1 *Be it enacted by the Senate and House of Representa-*
- 2 *tives of the United States of America in Congress assembled,*
- 3 That (a) the National Security Act of 1947 is amended by
- 4 adding at the end thereof the following new title:

1 "TITLE V—CLASSIFICATION AND SAFEGUARD-  
2 ING OF NATIONAL SECURITY INFORMATION

3 "PURPOSE

4 "SEC. 501. The purpose of this title is to establish pro-  
5 cedures for the protection against unauthorized disclosure of  
6 information and material relating to the national security that  
7 is of such a nature that the unauthorized disclosure of such  
8 information or material could cause identifiable damage to  
9 the national security and to provide criminal penalties for the  
10 unauthorized disclosure of such information and material.

11 "AUTHORITY FOR CLASSIFICATION OF NATIONAL  
12 SECURITY INFORMATION

13 "SEC. 502. (a) Except as provided in the Atomic  
14 Energy Act of 1954, national security information may be  
15 designated and protected against unauthorized disclosure  
16 only in accordance with this title. The authority to originate  
17 the classification of national security information may be ex-  
18 ercised only by an official designated under section 503 to  
19 have such authority and shall be exercised in accordance with  
20 the provisions of section 504.

21 "(b) There shall be three categories of classification by  
22 which national security information may be designated, and,  
23 except as otherwise expressly provided by law, no other cate-  
24 gory or degree of classification shall be used to identify or  
25 protect national security information. The three categories of

1 classification shall be known as Top Secret, Secret, and Con-  
2 fidential. National security information shall be designated by  
3 these categories as follows:

4           “(1) The classification ‘Top Secret’ shall be ap-  
5 plied to that national security information the unau-  
6 thorized disclosure of which reasonably could be ex-  
7 pected to cause exceptionally grave damage to the na-  
8 tional security.

9           “(2) The classification ‘Secret’ shall be applied to  
10 that national security information the unauthorized dis-  
11 closure of which reasonably could be expected to cause  
12 serious damage to the national security.

13           “(3) The classification ‘Confidential’ shall be ap-  
14 plied to that national security information the unau-  
15 thorized disclosure of which reasonably could be ex-  
16 pected to cause identifiable damage to the national  
17 security.

18           “OFFICIALS WITH AUTHORITY TO CLASSIFY NATIONAL  
19 SECURITY INFORMATION

20           “SEC. 503. (a)(1) The authority to originate the classifi-  
21 cation of national security information as ‘Top Secret’ may  
22 be exercised only by the President, by the heads of such  
23 agencies, and by such officials in the Executive Office of the  
24 President, as the President may designate by publication in  
25 the Federal Register to have such authority, and by such



1 officials as may be designated to have such authority in ac-  
2 cordance with subsection (b)(1).

3       “(2) The authority to originate the classification of na-  
4 tional security information as ‘Secret’ may be exercised only  
5 by officials who have authority to originate the classification  
6 of information as ‘Top Secret’, by such other officials in the  
7 executive branch of the Government as the President may  
8 designate by publication in the Federal Register to have such  
9 authority, and by such officials as may be designated to have  
10 such authority in accordance with subsection (b)(2).

11       “(3) The authority to originate the classification of na-  
12 tional security information as ‘Confidential’ may be exercised  
13 only by officials who have authority to originate the classifi-  
14 cation of information as ‘Secret’, by such other officials in the  
15 executive branch of the Government as the President may  
16 designate by publication in the Federal Register to have such  
17 authority, and by such officials as may be designated to have  
18 such authority in accordance with subsection (b)(3).

19       “(b)(1) Any principal subordinate official of an official  
20 designated by the President under subsection (a)(1) to have  
21 authority to originate the classification of information as ‘Top  
22 Secret’ may be designated by such official to have such au-  
23 thority, if such subordinate official has a frequent need to  
24 exercise such authority, as determined by the President or by  
25 the official making the designation.

1       “(2) Any subordinate official of an official who (A) has  
2 authority to designate information as ‘Top Secret’, or (B) is  
3 designated by the President under subsection (a)(2) to have  
4 authority to designate information as ‘Secret’ may be desig-  
5 nated by such official to have such authority if such subordi-  
6 nate official has a frequent need to exercise such authority, as  
7 determined by the President, by the head of such official’s  
8 agency, or by the official making the designation.

9       “(3) Any subordinate official of an official who (A) has  
10 authority to designate information as ‘Secret’, or (B) is desig-  
11 nated by the President under subsection (a)(3) to have  
12 authority to designate information as ‘Confidential’ may be  
13 designated by such official to have such authority if such sub-  
14 ordinate official has a frequent need to exercise such author-  
15 ity, as determined by the President, by the head of such offi-  
16 cial’s agency, or by some other official having authority to  
17 originate the classification of information as ‘Top Secret’.

18       “(4) Each designation under this subsection of an official  
19 to have authority to originate the classification of information  
20 shall be made in writing and shall state the name or position  
21 of the official being designated to exercise such authority.

22       “(c) It is the policy of the Congress that the number of  
23 designations under subsection (b) of subordinate officials to  
24 have authority to originate the classification of information  
25 should be kept to the smallest number practicable. To carry

1 out this policy, periodic reviews of such designations shall be  
2 made to determine whether officials so designated have a  
3 continuing need to exercise such authority.

4 “(d) The President shall prescribe regulations to provide  
5 procedures for the handling and classification of national se-  
6 curity information that is originated by an agency that does  
7 not have an official with authority to classify such  
8 information.

9 “STANDARDS FOR CLASSIFICATION

10 “SEC. 504. (a) Information may not be classified unless  
11 unauthorized disclosure of such information reasonably could  
12 be expected to cause at least identifiable damage to the na-  
13 tional security and unless such information concerns—

14 “(1) military plans, weapons, or operations;

15 “(2) information that is furnished to the United  
16 States by a foreign government or international organi-  
17 zation and that has been designated by such foreign  
18 government or international organization as requiring  
19 protection against unauthorized disclosure;

20 “(3) intelligence activities, sources, or methods;

21 “(4) the foreign relations or foreign activities of  
22 the United States;

23 “(5) scientific, technological, or economic matters  
24 relating to the national security;

1           “(6) programs of the United States Government  
2           for safeguarding nuclear materials or facilities; or

3           “(7) some other category of information related to  
4           the national security and requiring protection against  
5           unauthorized disclosure, as determined by the Presi-  
6           dent, by an official designated by the President under  
7           section 503(a)(1), or by an official who is the head of  
8           an agency.

9           “(b) The unauthorized disclosure of information de-  
10          scribed in subsection (a)(2) or of information revealing the  
11          identity of a confidential foreign intelligence source may be  
12          presumed to cause at least identifiable damage to the national  
13          security.

14          “(c)(1) Information may not be classified in order to con-  
15          ceal violations of law, incompetence, inefficiency, wrongdo-  
16          ing, or administrative error, to avoid embarrassment to any  
17          person or agency, to restrain competition or independent ini-  
18          tiative, or to prevent for any other reason the release of infor-  
19          mation that does not require protection in the interest of na-  
20          tional security. Any official who classifies information in vio-  
21          lation of this subsection shall be subject to such administra-  
22          tive disciplinary action, including suspension, as may be or-  
23          dered by such official's superiors.

24          “(2) Basic scientific research information not clearly re-  
25          lated to the national security may not be classified.

1       “(3) Material containing a reference to classified infor-  
2 mation which reference does not itself reveal classified infor-  
3 mation may not be classified by reason of such reference or  
4 be used as a basis for classification.

5       “(d) Whenever there is reasonable doubt as to which  
6 category of classification should be applied, the less restric-  
7 tive category should be used. Whenever there is reasonable  
8 doubt as to whether information should be classified at all,  
9 the information should not be classified.

10       “IDENTIFICATION OF CLASSIFIED MATERIAL

11       “SEC. 505. (a) Each item of classified material shall  
12 show on its face—

13               “(1) the category of classification of such material;

14               “(2) the identity of the official authorizing the  
15 original classification of such material;

16               “(3) the office which originated the classification  
17 of such material;

18               “(4) the dates of the preparation and of the classi-  
19 fication of such material; and

20               “(5) whether such material is subject to declassifi-  
21 cation at a particular time and, if so, when.

22       “(b) There shall be clearly indicated on the face of each  
23 item of classified material or by other appropriate means  
24 which portions of such material are classified and which por-  
25 tions are not classified, together with the degree of classifica-

1 tion of those portions which are classified. The President may  
2 waive the requirements of the preceding sentence for speci-  
3 fied classes of material.

4       “(c) Information that is furnished to the United States  
5 by a foreign government or international organization and  
6 that has been designated by such foreign government or  
7 international organization as requiring protection against un-  
8 authorized disclosure shall either retain its original designa-  
9 tion or be assigned a category of classification under this  
10 title, and in either case shall be assured a degree of protec-  
11 tion equivalent to that required by the foreign government or  
12 international organization furnishing such information.

13       “(d) A holder of classified information shall observe and  
14 respect the classification assigned to such information by the  
15 originator of such classification. If a holder of classified infor-  
16 mation believes that such information should not be classified,  
17 that the classification which has been assigned to such infor-  
18 mation is improper, or that such information is subject to  
19 declassification under applicable regulations, such holder  
20 shall so inform the originator of the classification of such in-  
21 formation, who shall promptly reexamine such classification.

22       “DECLASSIFICATION POLICY AND REGULATIONS

23       “SEC. 506. (a) It is the policy of the Congress that de-  
24 classification of classified information shall be given emphasis  
25 comparable to that accorded classification of national security

1 information. Information classified under this title or under a  
2 prior Executive order authorizing the classification of nation-  
3 al security information shall be declassified as early as con-  
4 siderations of national security allow.

5       “(b) The President shall prescribe regulations to estab-  
6 lish procedures for the systematic and periodic review of all  
7 classified information for the purpose of downgrading the  
8 classification of such information, or of declassifying, transfer-  
9 ring, retiring, or destroying such information, as may be ap-  
10 propriate in each case, at the earliest practicable date. In  
11 determining whether information should be declassified, the  
12 public interest in disclosure of the information shall be consid-  
13 ered and weighed against the need for continued classification  
14 of the information.

15                   “IMPLEMENTING REGULATIONS

16       “SEC. 507. (a) The President shall prescribe regulations  
17 to carry out this title. Such regulations shall include provi-  
18 sions to ensure that—

19               “(1) any person given access to classified informa-  
20 tion (A) has been determined to be trustworthy, and  
21 (B) requires access to such information in the perform-  
22 ance of official duties;

23               “(2) all classified material is appropriately and  
24 conspicuously marked so as to put any person coming

1 in contact with such material on clear notice that the  
2 contents of such material are classified;

3 “(3) classified information is used, possessed,  
4 stored, reproduced, and transmitted only under condi-  
5 tions that will prevent access to such information by  
6 persons not specifically authorized to have such access  
7 and that will prevent dissemination of such information  
8 to persons not specifically authorized to receive it;

9 “(4) classified information disseminated outside  
10 the executive branch is given protection equivalent to  
11 that afforded within the executive branch;

12 “(5) appropriate records to assure accountability  
13 for all classified information are established and main-  
14 tained and that classified information is adequately pro-  
15 tected during all transmissions of such information; and

16 “(6) classified information no longer needed in  
17 current working files or for reference or record pur-  
18 poses is destroyed or otherwise disposed of in accord-  
19 ance with chapter 33 of title 44, United States Code  
20 (relating to disposal of records).

21 “(b) The President may waive the requirement in sub-  
22 section (a)(1) that access to classified information be limited  
23 to persons requiring access to such information in the per-  
24 formance of official duties with respect to such persons and  
25 classes of persons as the President may prescribe.



1 "MATERIAL COVERED BY THE ATOMIC ENERGY ACT OF  
2 1954

3 "SEC. 508. Nothing in this title shall supersede any re-  
4 quirement made by or under the Atomic Energy Act of 1954.  
5 Material designated as 'Restricted Data' and material desig-  
6 nated as 'Formerly Restricted Data' shall be handled, pro-  
7 tected, classified, downgraded, and declassified in conformity  
8 with the provisions of the Atomic Energy Act of 1954.

9 "UNAUTHORIZED DISCLOSURE OF CLASSIFIED  
10 INFORMATION

11 "SEC. 509. (a) Any individual who knowingly communi-  
12 cates classified information which that individual knows or  
13 has reason to know is classified information to a foreign gov-  
14 ernment or foreign organization or to any officer or agent  
15 thereof not authorized to receive such information shall be  
16 imprisoned for any term of years or for life.

17 "(b) Any individual who (1) is or has been in authorized  
18 possession or control of classified information, or (2) is or has  
19 been an officer or employee of the United States, a member  
20 of the Armed Forces of the United States, a contractor of the  
21 United States Government, or an employee of a contractor of  
22 the United States Government, and is or has been in posses-  
23 sion or control of classified information in the course of that  
24 relationship, knowingly communicates such information to a

1 person not authorized to receive it shall be fined not more  
2 than \$10,000 or imprisoned not more than ten years, or both.

3       “(c) Any individual who knowingly communicates clas-  
4 sified information which that individual knows or has reason  
5 to know is classified information to a person not authorized to  
6 receive it shall be fined not more than \$5,000 or imprisoned  
7 not more than one year, or both. Nothing in this subsection  
8 shall be construed to infringe rights or liberties guaranteed  
9 under the Constitution or laws of the United States.

10       “(d) It is a defense to a prosecution under subsection (b)  
11 or (c) that—

12               “(1) before the commission of the offense with  
13 which the defendant is charged, the information com-  
14 municated had been publicly disclosed;

15               “(2) the information communicated was not law-  
16 fully classified at the time of the offense with which  
17 the defendant is charged; or

18               “(3) the information communicated was communi-  
19 cated only to a regularly constituted subcommittee,  
20 committee, or joint committee of Congress, pursuant to  
21 lawful demand.

22       “(e) In making a determination as to whether the infor-  
23 mation communicated was lawfully classified at the time of  
24 the offense with which the defendant is charged, the court  
25 shall determine the matter and shall examine such informa-

1 tion in camera. In any such determination, the burden is on  
2 the United States to sustain the classification of such infor-  
3 mation. After any in camera examination under this subsec-  
4 tion, the court shall enter into the record its findings and  
5 determinations with respect to whether the information com-  
6 municated was lawfully classified at the time of the offense  
7 with which the defendant is charged. Any determination by  
8 the court under this subsection shall be a question of law.

9       “(f)(1) Whenever any person is about to engage in con-  
10 duct that would constitute a violation of this section, the At-  
11 torney General, on behalf of the United States, may apply to  
12 the appropriate court for an order enjoining such conduct,  
13 and upon a showing that a person is about to engage in such  
14 conduct, a permanent or temporary injunction, temporary re-  
15 straining order, or other order may be granted.

16       “(2) In making a determination as to whether a viola-  
17 tion of this section is about to occur, the court shall examine  
18 the information that is the subject of the possible violation  
19 and shall not grant relief under this subsection if the informa-  
20 tion is not lawfully classified. Examination of the contents of  
21 such information shall be conducted in camera. In any such  
22 determination, the burden is on the United States to sustain  
23 the classification of such information. After an in camera ex-  
24 amination under this subsection, the court shall enter into the

1 record its findings and determinations with respect to wheth-  
2 er the information is lawfully classified.

3 “(g) For the purposes of this section:

4 “(1) The term ‘classified information’ means infor-  
5 mation that is designated as information that—

6 “(A) has been classified under this title;

7 “(B) was classified before the effective date  
8 of this title under an Executive order; or

9 “(C) was furnished to the United States by a  
10 foreign government or international organization  
11 and was designated by such foreign government  
12 or international organization as requiring protec-  
13 tion against unauthorized disclosure.

14 “(2) The term ‘communicates’ means to impart,  
15 transfer, publish, or otherwise make available.

16 “(3) The term ‘authorized’, when used in relation  
17 to the possession, receipt, or control of classified infor-  
18 mation, means with legal authority to have access to,  
19 to possess, to receive, or to control such information.

20 “(4) The term ‘lawfully classified’, when used in  
21 relation to classified information, means—

22 “(A) in the case of information classified on  
23 or after the effective date of this title, that such  
24 information—

1                   “(i) is specifically authorized under the  
2 criteria established by section 504 to be clas-  
3 sified;

4                   “(ii) is in fact properly classified and  
5 identified in accordance with the criteria es-  
6 tablished by sections 504 and 505 and regu-  
7 lations issued under section 507; and

8                   “(iii) was classified by an official author-  
9 ized under section 503 to make such a clas-  
10 sification;

11                   “(B) in the case of information classified  
12 before the effective date of this title, that such in-  
13 formation—

14                   “(i) is specifically authorized under cri-  
15 teria established by an Executive order to be  
16 protected from unauthorized disclosure in the  
17 interest of the national security;

18                   “(ii) is in fact properly classified under  
19 the criteria and procedures established by  
20 such Executive order; and

21                   “(iii) was classified by a person author-  
22 ized by statute, Executive order, or regula-  
23 tion to make such a classification; and

24                   “(C) in the case of information designated as  
25 information which (i) was furnished to the United

1       States by a foreign government or international  
2       organization, and (ii) was designated by such for-  
3       foreign government or international organization as  
4       requiring protection against unauthorized disclo-  
5       sure, that such information was in fact furnished  
6       to the United States by a foreign government or  
7       international organization and was in fact desig-  
8       nated by such foreign government or international  
9       organization as requiring protection from unau-  
10      thorized disclosure.

11                “PENALTY FOR IMPROPER CLASSIFICATION

12       “SEC. 510. Whoever classifies information in order to  
13      conceal incompetence, inefficiency, wrongdoing, or adminis-  
14      trative error, to avoid embarrassment to any individual or  
15      agency, to restrain competition or independent initiative, or  
16      to prevent or delay for any reason the release of information  
17      which does not bear directly on the effectiveness of the na-  
18      tional defense or the conduct of foreign relations shall be  
19      fined not more than \$1,000 or imprisoned not more than one  
20      year, or both.

21                “DEFINITIONS

22       “SEC. 511. For purposes of this title:

23       “(1) The term ‘national security information’  
24      means information and material that is owned by, pro-  
25      duced for or by, or under the control of the United

1 States Government and that requires protection against  
2 unauthorized disclosure for reasons of the national se-  
3 curity.

4 “(2) The term ‘national security’ means the na-  
5 tional defense or foreign relations of the United States.

6 “(3) The term ‘information’ includes material con-  
7 taining information.

8 “(4) The term ‘agency’ means any executive de-  
9 partment, military department, Government corpora-  
10 tion, Government-controlled corporation, or other es-  
11 tablishment in the executive branch of the Government  
12 (including the Executive Office of the President), or  
13 any independent regulatory agency.”.

14 (b) The table of contents at the beginning of the Nation-  
15 al Security Act of 1947 is amended by adding at the end  
16 thereof the following:

“TITLE V—CLASSIFICATION AND SAFEGUARDING OF NATIONAL SECURITY  
INFORMATION

“Sec. 501. Purpose.

“Sec. 502. Authority for classification of national security information.

“Sec. 503. Officials with authority to classify national security information.

“Sec. 504. Standards for classification.

“Sec. 505. Identification of classified material.

“Sec. 506. Declassification policy and regulations.

“Sec. 507. Implementing regulations; standards.

“Sec. 508. Material covered by the Atomic Energy Act of 1954.

“Sec. 509. Unauthorized disclosure of classified information.

“Sec. 510. Penalty for improper classification.

“Sec. 511. Definitions.”.

17 SEC. 2. The amendments made by the first section of  
18 this Act shall take effect at the end of the ninety-day period  
19 beginning on the date of the enactment of this Act.